

On L -functions and the Selberg Class

J. Stuart Hutchison

May 21, 2010

1 Introduction

The purpose of this thesis will be to explore the relationship between elliptic curves and L -functions. We will start off with a section giving some necessary definitions that will be used throughout the entire paper. Following this will be a section on the Selberg class of L -functions. These two chapters serve as the setup to the rest of the paper. As we will see in the Selberg section, for an L -function to be in the Selberg class it must satisfy a select few properties. So, moving from elliptic curves to modular forms we will show how the L -function associated to a modular form will actually satisfy all these conditions. Thus, the entire point of the paper can be summed up as: the L -function for a modular form belongs to the Selberg class. We will conclude with a section explaining why the Selberg Class L -functions are important.

2 Preliminary Definitions

This section will introduce most of the core concepts that will be used throughout the paper. There are a few proofs here but they will mainly be used as a way to further expand on and elaborate on these new terms. Other definitions will certainly appear in the other sections but usually their purpose is served in a limited capacity. The definitions here are instead used frequently in the other sections.

This section will be split up into two parts. The first part will be for basic definitions regarding elliptic curves on the complex plane and modular functions. The second part will be for definitions more in line with the L -function side of the paper.

2.1 Elliptic Curves

While we will not really be working with elliptic curves themselves, many of the objects we will be working with are strongly connected with elliptic curves. Therefore, I feel it necessary to start everything off with the definition of an elliptic curve.

Definition 1. Let K be an arbitrary field. An elliptic curve E/K is a smooth projective curve of genus 1 over K together with a point $\mathcal{O} \in E(K)$.

We usually write elliptic curves in the following way (the coefficients look weird, but were chosen for other reasons which I will not get into):

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Usually, these elliptic curves are defined over certain fields such as \mathbb{R} or \mathbb{C} or even a p -adic field. When defined over \mathbb{C} it's important to have a lattice that will serve as a basis for the curve.

Definition 2. A lattice is a subset of \mathbb{C} of the following form: $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{n_1\omega_1 + n_2\omega_2 \mid n_i \in \mathbb{Z}, \omega_i \in \mathbb{C}; \omega_1, \omega_2 \text{ } \mathbb{R}\text{-linearly independent}\}$. We call ω_1 and ω_2 the basis elements of our lattice.

Because of the way we order ω_1 and ω_2 (the angle from ω_2 to ω_1 must be positive and between 0 and π since they are \mathbb{R} -linearly independent) we can assume that $\text{Im}(\omega_1/\omega_2) > 0$ and we can normalize our basis to get $\frac{1}{\omega_2}\Lambda = \mathbb{Z}\frac{\omega_1}{\omega_2} + \mathbb{Z}$. This is because we really only care about homothetic lattices (in short, lattices are homothetic if there is a $k \in \mathbb{C}^\times$ such that $\Lambda_1 = k\Lambda_2$). We now have the following proposition:

Proposition 1. 1. Let $\Lambda \in \mathbb{C}$ be a lattice and let ω_1, ω_2 and ω'_1, ω'_2 be two oriented bases for Λ . Then:

$$\omega'_1 = a\omega_1 + b\omega_2 \quad \text{and} \quad \omega'_2 = c\omega_1 + d\omega_2$$

for some matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$.

2. Let $\Lambda \in \mathbb{C}$ be a lattice. Then there is a $\tau \in \mathbb{H}$ such that Λ is homothetic to $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$.

3. Let $\tau_1, \tau_2 \in \mathbb{H}$. Then Λ_{τ_1} is homothetic to Λ_{τ_2} if and only if there is a matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \quad \text{such that} \quad \tau_1 = \frac{a\tau_2 + b}{c\tau_2 + d}.$$

Proof. 1. If we have both ω_1, ω_2 and ω'_1, ω'_2 serving as oriented bases for Λ then we get:

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \mathbb{Z}\omega'_1 + \mathbb{Z}\omega'_2.$$

Using the definition of an oriented basis:

$$\begin{aligned} \omega_1 &= a'\omega'_1 + b'\omega'_2 & \omega'_1 &= a\omega_1 + b\omega_2 \\ \omega_2 &= c'\omega'_1 + d'\omega'_2 & \omega'_2 &= c\omega_1 + d\omega_2 \end{aligned}$$

where $a, b, c, d, a', b', c', d' \in \mathbb{Z}$. Now, using substitution and the fact that ω_1 and ω_2 are \mathbb{R} -linearly independent, we get:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Next, via the use of an identity and our bases being oriented we get:

$$0 < \operatorname{Im} \left(\frac{\omega'_1}{\omega'_2} \right) = \operatorname{Im} \left(\frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2} \right) = \frac{(ad - bc)\operatorname{Im}(\omega_1/\omega_2)}{|c(\omega_1/\omega_2) + d|^2}.$$

Therefore we have that $ad - bc > 0$ and thus $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. This proves the first part.

2. This part is trivial. We just let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ where ω_1, ω_2 constitute an oriented basis. Then simply take $\tau = \omega_1/\omega_2$.
3. First assume that Λ_{τ_1} is homothetic to Λ_{τ_2} . Then we have that

$$\mathbb{Z}\tau_1 + \mathbb{Z} = \alpha(\mathbb{Z}\tau_2 + \mathbb{Z}) \quad \text{for some } \alpha \in \mathbb{C}^\times.$$

But then, from the previous part we get that:

$$\tau_1 = \alpha(a\tau_2 + b) \quad \text{and} \quad 1 = \alpha(c\tau_2 + d) \quad \text{for some } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

But then we have $\tau_1 = \frac{a\tau_2 + b}{c\tau_2 + d}$ which is exactly what we wanted to show.

Now, for the other direction. Assume that $\tau_1 = \frac{a\tau_2 + b}{c\tau_2 + d}$. Let $\alpha = c\tau_2 + d$. Next, again using the first part, we discover that

$$\alpha\Lambda_{\tau_1} = \alpha(\mathbb{Z}((a\tau_2 + b)/(c\tau_2 + d)) + \mathbb{Z}) = \mathbb{Z}\tau_2 + \mathbb{Z} = \Lambda_{\tau_2}$$

which shows that Λ_{τ_1} and Λ_{τ_2} are homothetic. □

We now introduce another definition related to lattices, mainly what it means for a lattice Λ to be a *sublattice of index n* .

Definition 3. Let $ad - bc = n$ and let ω_1, ω_2 be an oriented basis for Λ . Then if

$$\Lambda' = \mathbb{Z}(a\omega_1 + b\omega_2) + \mathbb{Z}(c\omega_1 + d\omega_2)$$

we say that Λ' is a sublattice of Λ of index n . The following notations will be used for this: $[\Lambda : \Lambda'] = n$ or $\Lambda' \overset{n}{\subset} \Lambda$.

For many parts of this paper we will be working with the following group:

Definition 4. The modular group, denoted $\Gamma(1)$ is the quotient group:

$$\Gamma(1) = SL_2(\mathbb{Z})/\{\pm 1\}.$$

And in the same vein, we introduce modular functions:

Definition 5. Let $k \in \mathbb{Z}$, and let $f(\tau)$ be a function on \mathbb{H} . We say that f is weakly modular of weight $2k$ (for $\Gamma(1)$) if the following condition is satisfied:

$$f(\gamma\tau) = (c\tau + d)^{2k} f(\tau) \quad \text{for all } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1), \tau \in \mathbb{H}.$$

Definition 6. A weakly modular function that is meromorphic on $\mathbb{H} \cup \infty$ is called a modular function.

Definition 7. A modular function that is everywhere holomorphic (i.e. everywhere on \mathbb{H} and also at ∞) is called a modular form. If we also have that $f(\infty) = 0$, then f is called a cusp form.

Definition 8. Any such function that maps from \mathcal{L} to \mathbb{C} will be called a lattice function.

We finish this subsection up with a lemma relating some of these concepts.

Lemma 1. There is a one-to-one correspondence between the weakly modular functions $f : \mathbb{H} \rightarrow \mathbb{C}$ of weight $2k$ and the lattice functions $F : \mathcal{L} \rightarrow \mathbb{C}$ satisfying $F(\lambda\Lambda) = \lambda^{-2k}F(\Lambda)$ for all $\lambda \in \mathbb{C}^\times$. We have the following maps:

$$f \mapsto F_f(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2) = \omega_2^{-2k} f(\omega_1/\omega_2) \quad \text{and} \quad F \mapsto f_F(\tau) = F(\Lambda_\tau).$$

Proof. First we need to clarify what is going on with $F_f(\Lambda)$. As we can define Λ in a variety of ways, we need to make sure that $F_f(\Lambda)$ really does not depend on which basis we use. So, assume we are actually using the oriented basis $(a\omega_1 + b\omega_2, c\omega_1 + d\omega_2)$ for some $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. Thus:

$$\begin{aligned} F_f(\mathbb{Z}(a\omega_1 + b\omega_2) + \mathbb{Z}(c\omega_1 + d\omega_2)) &= (c\omega_1 + d\omega_2)^{-2k} f\left(\frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2}\right) \\ &= (c\omega_1 + d\omega_2)^{-2k} \left(c\frac{\omega_1}{\omega_2} + d\right)^{2k} f\left(\frac{\omega_1}{\omega_2}\right) \\ &= \omega_2^{-2k} f\left(\frac{\omega_1}{\omega_2}\right) = F_f(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2). \end{aligned}$$

So from this we see that the basis selected (from the class of bases) does not matter. Next, we see through a similar calculation that:

$$F_f(\lambda\Lambda) = F_f(\mathbb{Z}\lambda\omega_1 + \mathbb{Z}\lambda\omega_2) = \lambda^{-2k}F_f(\Lambda).$$

Finally, let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, then:

$$\Lambda_{\gamma\tau} = (c\tau + d)^{-1}(\mathbb{Z}(a\tau + b) + \mathbb{Z}(c\tau + d)) = (c\tau + d)^{-1}\Lambda_\tau$$

which gives

$$f_F(\gamma\tau) = F(\Lambda_{\gamma\tau}) = F((c\tau + d)^{-1}\Lambda_\tau) = (c\tau + d)^{2k}F(\Lambda_\tau) = (c\tau + d)^{2k}f_F(\tau).$$

Thus we have well defined maps. The final step is to see that the two maps are inverses of one another. We do simply by using the properties of the maps themselves and by using the fact that we are working with weakly modular functions.

$$\begin{aligned} F_{f_F}(\Lambda) &= \omega_2^{-2k} f_F\left(\frac{\omega_1}{\omega_2}\right) = \omega_2^{-2k} F(\Lambda_{\omega_1/\omega_2}) \\ &= \omega_2^{-2k} F\left(\mathbb{Z}\frac{\omega_1}{\omega_2} + \mathbb{Z}\right) = F(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2) = F(\Lambda). \\ f_{F_f}(\tau) &= F_f(\Lambda_\tau) = F_f(\mathbb{Z}\tau + \mathbb{Z}) = f(\tau) \end{aligned}$$

We then have the desired one-to-one correspondence which completes the proof of the lemma. \square

With that we conclude this section of definitions and turn our attention to the preliminary definitions for L -functions.

2.2 L -functions

To really describe what an L -function is we need to first define another term.

Definition 9. A group homomorphism $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \rightarrow S^1$ (where S^1 is the set of complex numbers with absolute value 1) such that $\chi(n) = 0$ whenever $\gcd(m, n) \neq 1$ is called a Dirichlet character.

Definition 10. For a Dirichlet character χ , the Dirichlet L -function (of χ) is

$$L(\chi, s) = \sum_{n \geq 1} \frac{\chi(n)}{n^s}.$$

Note that in this paper, the simpler term L -function is used.

Note immediately from basic complex analysis that $L(\chi, s)$ converges absolutely for $s > 1$ (in fact for $\operatorname{Re}(s) > 1$). This is important as we will see below.

We now move on to what it means for an L -function to be in the Selberg Class.

3 Being in the Selberg Class

For an L -function to be in the Selberg Class it must satisfy some selected properties. As I have mentioned above, the goal of this paper is to show how the L -function associated to a modular form will actually belong to the Selberg Class.

Definition 11. The Selberg class \mathcal{S} consists of the functions $f(s)$ satisfying the following conditions:

1. For $\operatorname{Re}(s) > 1$, $f(s)$ is an absolutely convergent Dirichlet series:

$$f(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}.$$

2. For some integer $m \geq 0$ the function $(s-1)^m f(s)$ extends by analytic continuation to an entire function. This property will simply be referred to as analytic continuation.

3. $f(s)$ satisfies a functional equation of the form

$$\Phi(s) = \omega \bar{\Phi}(1-s)$$

where

$$\Phi(s) = Q^s \prod_{j=1}^r \Gamma(\lambda_j s + \mu_j) f(s)$$

with $Q > 0, \lambda_j > 0, \operatorname{Re}(\mu_j) \geq 0$ and $|\omega| = 1$. This is called the functional equation.

4. For every $\epsilon > 0, a(n) \ll n^\epsilon$. This is called the Ramanujan hypothesis.

5. For $\operatorname{Re}(s)$ sufficiently large,

$$\log f(s) = \sum_{n=1}^{\infty} \frac{b(n)}{n^s}$$

where $b(n) = 0$ unless n is a positive power of a prime and $b(n) \ll n^\theta$ for some $\theta < \frac{1}{2}$. This is called the Euler product.

Now to go over what the "plan of attack" will be for the overall proof. First we have already seen that we can move from an elliptic curve to a modular form by way of Lemma 1. Thus we can from here on out be working exclusively with modular forms and their L -functions.

Concerning how these L -functions fit into the Selberg Class we note that in the previous section we noted the first property which followed trivially from our definitions. In the next section we will work on the fifth property, the Euler product. Finally, in the fifth section we will get the more analytic properties: analytic continuation, the functional equation, and the Ramanujan hypothesis.

4 Hecke Operators and the Euler Product Property

In this chapter I will go over what exactly a Hecke operator is and why it will be important to us. Eventually, we'll use the objects introduced here to arrive at a theorem relating the Hecke operators to the Euler product of the associated L -function. As mentioned above, this is one of the requirements to show that our given L -function is in the Selberg Class.

But way before we can do that we first have a preliminary definition for a *correspondence*.

Definition 12. For any set S , let $\operatorname{Div}(S)$ denote the divisor group of the set S , that is, the free abelian group generated by the elements of S ,

$$\operatorname{Div}(S) = \bigoplus_{s \in S} \mathbb{Z} \cdot s.$$

A homomorphism $T: \operatorname{Div}(S) \rightarrow \operatorname{Div}(S)$ is called a correspondence on S .

Now that we have that, we can introduce *Hecke operators* themselves.

Definition 13. Let $n \geq 1$ be an integer. The n^{th} Hecke operator $T(n)$ is the correspondence on the set of lattices \mathcal{L} whose value at a lattice $\Lambda \in \mathcal{L}$ is:

$$T(n)\Lambda = \sum_{\substack{\Lambda' \subset \Lambda \\ [\Lambda:\Lambda'] = n}} (\Lambda').$$

Next, we need to define another term, the *homothety operator* which will be used with the Hecke operators and lattices to establish some groundwork in an important theorem.

Definition 14. Let $\lambda \in \mathbb{C}^\times$. The homothety operator R_λ is the correspondence on \mathcal{L} whose value at a lattice $\Lambda \in \mathcal{L}$ is $R_\lambda\Lambda = \lambda\Lambda$.

Now that we have defined some more terms we can have our first big theorem which relates these two concepts.

Theorem 1. Given homothety operators R and Hecke operators $T(n)$:

1. $R_\lambda R_\mu = R_{\lambda\mu}$ for all $\lambda, \mu \in \mathbb{C}^\times$.
2. $R_\lambda T(n) = T(n) R_\lambda$ for all $\lambda \in \mathbb{C}^\times, n \geq 1$.
3. $T(mn) = T(m)T(n)$ for all $m, n \geq 1$ with $\gcd(m, n) = 1$.
4. $T(p^e)T(p) = T(p^{e+1} + pT(p^{e-1}))R_p$ for p prime, $e \geq 1$.

Proof. 1. Here we just simply look at the following string of equalities:

$$R_\lambda R_\mu(\Lambda) = R_\lambda(\mu\Lambda) = \lambda\mu\Lambda = R_{\lambda\mu}(\Lambda).$$

2. Next, for this part we recall the definitions of lattices. So: Λ' is a sublattice of Λ of index n if and only if $\lambda\Lambda'$ is a sublattice of $\lambda\Lambda$ of index n . Basically this follows from adding an extra λ to the definition where necessary.
3. Let $[\Lambda : \Lambda''] = mn$. Now, since $\gcd(m, n) = 1$ we can actually get a unique intermediate lattice Λ' with the following relation:

$$\Lambda'' \stackrel{m}{\subset} \Lambda' \stackrel{n}{\subset} \Lambda.$$

So from this we can get the desired result:

$$\begin{aligned} T(mn)\Lambda &= \sum_{\Lambda'' \stackrel{mn}{\subset} \Lambda} (\Lambda'') = \sum_{\Lambda' \stackrel{n}{\subset} \Lambda} \sum_{\Lambda'' \stackrel{m}{\subset} \Lambda'} (\Lambda'') \\ &= \sum_{\Lambda' \stackrel{n}{\subset} \Lambda} T(m)(\Lambda') = T(m) \sum_{\Lambda' \stackrel{n}{\subset} \Lambda} (\Lambda') = T(m)T(n)\Lambda. \end{aligned}$$

So basically this amounted to just taking a sum, splitting it up and then rearranging it in a certain way. This proves the desired result.

4. First let $\Lambda \in \mathcal{L}$. Let $\Lambda' \stackrel{p^{e+1}}{\subset} \Lambda$. We introduce the following two integers:

$$a(\Lambda') = \#\{\Gamma \mid \Lambda' \subset \Gamma \stackrel{p}{\subset} \Lambda\};$$

$$b(\Lambda') = \{1 \text{ if } \Lambda' \subset p\Lambda \text{ and } 0 \text{ otherwise}\}.$$

Then we have the following:

$$\begin{aligned} T(p^e)T(p)\Lambda &= \sum_{\Gamma \stackrel{p}{\subset} \Lambda} \sum_{\Lambda' \stackrel{p^e}{\subset} \Gamma} (\Lambda') = \sum_{\Lambda' \stackrel{p^{e+1}}{\subset} \Lambda} a(\Lambda')(\Lambda') \\ T(p^{e+1})\Lambda &= \sum_{\Lambda' \stackrel{p^{e+1}}{\subset} \Lambda} (\Lambda') \\ T(p^{e-1})\Lambda &= \sum_{\Lambda'' \stackrel{p^{e-1}}{\subset} p\Lambda} (\Lambda'') = \sum_{\Lambda' \stackrel{p^{e+1}}{\subset} \Lambda} b(\Lambda')(\Lambda'). \end{aligned}$$

Now, when we compare this to (4) we see that we have to prove the following:

$$a(\Lambda') = 1 + pb(\Lambda') \text{ for all } \Lambda' \stackrel{p^{e+1}}{\subset} \Lambda.$$

Our first case is when $\Lambda' \subset p\Lambda$ and $b(\Lambda') = 1$. First let $\Gamma \stackrel{p}{\subset} \Lambda$. Then we have that $\Lambda' \subset p\Lambda \subset \Gamma$ and so we must count these Γ . Thus we get that $a(\Lambda') = \#\{\Gamma \mid \Gamma \stackrel{p}{\subset} \Lambda\} = 1 + p$. But this is the same as the $1 + pb(\Lambda')$ as required.

Our second case is for Λ' not a subset of $p\Lambda$ and for $b(\Lambda') = 0$. First, for our second case we let Γ be a lattice such that $\Lambda' \subset \Gamma \stackrel{p}{\subset} \Lambda$. Then:

$$0 \subsetneq \frac{\Lambda'}{\Lambda' \cap p\Lambda} \subseteq \frac{\Gamma}{p\Lambda} \stackrel{p}{\subset} \frac{\Lambda}{p\Lambda}.$$

However, we recall that $\Lambda/p\Lambda$ has order p^2 . Therefore, the center containment must be an equality. From this we see that

$$\Gamma = \Lambda' + p\Lambda.$$

Therefore for our given Λ' we obtain only one such Γ satisfying the restrictions. Then since $a(\Lambda') = 1$ and $b(\Lambda') = 0$ we get $a(\Lambda') = 1 + pb(\Lambda')$ as desired.

With both of these cases being proved we have completed the proof of this final part of the theorem. □

Next, we have a corollary which also introduces another definition.

Corollary 1. *We have the following isomorphism of rings:*

$$\mathbb{Z}[T(n), R_n \mid n \in \mathbb{Z}, n \geq 1] \cong \mathbb{Z}[T(p), R_p \mid p \text{ prime}].$$

This shows that every $T(n)$ is a polynomial in the $T(p)$'s and R_p 's for primes p . For simplicity we call these two rings the Hecke algebra (of $\Gamma(1)$).

Proof. First we factor n as $n = p_1^{e_1} \cdots p_r^{e_r}$. Now, we use the previous Theorem 1 to split up R_n and $T(n)$ as follows:

$$R_n = \prod_{i=1}^r R_{p_i}^{e_i} \quad \text{and} \quad T(n) = \prod_{i=1}^r T(p_i^{e_i}).$$

Now we induct on e using Theorem 1.

For our base case we have $e = 1$ in which case we just have $T(p^1)$ which is automatically a polynomial in $T(p)$ and R_p . So now let $e \geq 1$ and apply induction. We have $T(p^{e+1}) = T(p^e)T(p) - pT(p^{e-1})R_p$ from the theorem. By the base case we have $T(p)$ as required and from the inductive hypothesis we have $T(p^e)$ as required. Thus we get the desired result: $T(p^{e+1})$ can be written as polynomial of $T(p)$'s and R_p 's. \square

Corollary 2. *The Hecke algebra $\mathbb{Z}[T(n), R_n \mid n \in \mathbb{Z}, n \geq 1]$ is commutative. Thus we get, for all $m, n \geq 1$ that $T(m)T(n) = T(n)T(m)$.*

Proof. This again follows from the results shown in Theorem 1. From there we recall that $T(mn) = T(m)T(n)$ for all $m, n \geq 1$ with $\gcd(m, n) = 1$. Thus we only need to verify the result for the cases of $T(p^e)$ and $T(p^f)$. However, from the above Corollary 1 we get that $T(p^e)$ is a polynomial in $T(p)$ and R_p . But this also holds true for $T(p^f)$. And now, again from Theorem 1, we know that these commute. Therefore we get the entire commutativity as required. \square

Now we need to find a way to tie some of these concepts together. Basically, we're going to see that Hecke operators behave similar to how the coefficients of the L -function do and from this we'll end up getting the Euler product. For now, we will look at how they operate on lattices. First, some notation:

Notation 1. *Let $n \geq 1$ be an integer. We define the following two objects:*

$$\begin{aligned} \mathcal{D}_n &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \mid ad - bc = n \right\}, \\ \mathcal{S}_n &= \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_2(\mathbb{Z}) \mid ad = n; a, d > 0; 0 \leq b < d \right\}. \end{aligned}$$

Lemma 2. *Let $\Lambda \in \mathcal{L}$ be a lattice, and let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be an oriented basis for Λ . Then the Hecke operator $T(n)$ is given explicitly by the formulas*

$$T(n)\Lambda = \sum_{\substack{ad=n, a \geq 1 \\ a \leq b \leq d}} (\mathbb{Z}(a\omega_1 + b\omega_2) + \mathbb{Z}d\omega_2) = \sum_{\alpha \in \mathcal{S}_n} (\alpha(\Lambda)).$$

Here we define $\alpha(\Lambda)$ as $\alpha(\Lambda) = \mathbb{Z}(a\omega_1 + b\omega_2) + \mathbb{Z}(c\omega_1 + d\omega_2)$.

Proof. Our real goal here is to show that there is a one-to-one correspondence between $SL_2 \backslash \mathcal{D}_n$ and $\{\Lambda' : \Lambda' \overset{n}{\subset} \Lambda\}$. As we have seen from the definition of Hecke operators acting on lattices, we get that $T(n)$ sends Λ to a sum of sublattices, each of degree n with respect to Λ . So, we now let $\Lambda \in \mathcal{L}$, and let Λ be given by $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ as usual (an oriented basis). Now let $\Lambda' \overset{n}{\subset} \Lambda$ and let Λ' be similarly given by $\mathbb{Z}\omega'_1 + \mathbb{Z}\omega'_2$ where we have $\omega'_1 = a\omega_1 + b\omega_2$ and $\omega'_2 = c\omega_1 + d\omega_2$ with $a, b, c, d \in \mathbb{Z}$. Now we get:

$$n = [\Lambda : \Lambda'] = \frac{\text{Area of } \alpha D}{\text{Area of } D} = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$$

where D is a fundamental parallelogram of \mathbb{C}/Λ . Thus we have half of the required map, namely:

$$\{\alpha \in M_2\mathbb{Z} \mid \det(\alpha) = n\} \rightarrow \{\Lambda' : \Lambda' \overset{n}{\subset} \Lambda\}$$

with $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \alpha(\Lambda) = \mathbb{Z}(a\omega_1 + b\omega_2) + \mathbb{Z}(c\omega_1 + d\omega_2)$.

Finally, we have to verify that we cannot get the same sublattice mapped to by multiple α 's. However, we see this by recalling that $\alpha(\Lambda) = \alpha'(\Lambda)$ if and only if $\alpha = \gamma\alpha'$ for some $\gamma \in SL_2(\mathbb{Z})$. Thus we get that the sublattices of Λ of index n are precisely the lattices of $\alpha(\Lambda)$ with $\alpha \in \mathcal{S}_n$. \square

Moving on from Hecke operators on lattices we want to turn our focus to Hecke operators on modular forms. Again keep in mind that the end result we really want from all this is to get an Euler product by use of our Hecke operators.

Definition 15. The n^{th} Hecke operator $T_{2k}(n)$ on the space of modular functions of weight $2k$ is defined by the formula:

$$(T_{2k}(n)f)(\tau) = n^{2k-1} \sum_{\Lambda' \overset{n}{\subset} \Lambda_\tau} F_f(\Lambda') = n^{2k-1} \sum_{\substack{ad=n, a \geq 1 \\ 0 \leq b < d}} d^{-2k} f\left(\frac{a\tau + b}{d}\right).$$

This definition is important because it ties together Hecke operators on lattices (recall the properties of Lemma 1) with Hecke operators on modular forms.

Lemma 3. Let $f(\tau) = \sum c(m)q^m$ be a modular function of weight $2k$. Then the Fourier series for $T_{2k}(n)f$ is

$$(T_{2k}(n)f)(\tau) = \sum_{m \in \mathbb{Z}} \gamma(m)q^m, \quad \text{where } \gamma(m) = \sum_{a \mid \gcd(m, n)} a^{2k-1} c\left(\frac{mn}{a^2}\right).$$

Note that here we are using the standard notation where $q = e^{i2\pi\tau}$, a complex variable on the unit disk in the upper half plane (since τ is restricted to \mathbb{H}).

Proof. Recall the formula for $T_{2k}(n)f$:

$$\begin{aligned}
(T_{2k}(n)f)(\tau) &= n^{2k-1} \sum_{\substack{ad=n; a \geq 1 \\ 0 \leq b < d}} d^{-2k} f\left(\frac{a\tau + b}{d}\right) \\
&= n^{2k-1} \sum_{\substack{ad=n; a \geq 1 \\ 0 \leq b < d}} d^{-2k} \sum_{m \in \mathbb{Z}} c(m) e^{i2\pi m(a\tau + b)/d} \\
&= n^{2k-1} \sum_{m \in \mathbb{Z}} \sum_{ad=n; a \geq 1} c(m) d^{-2k} e^{i2\pi ma\tau/d} \sum_{0 \leq b < d} e^{i2\pi mb/d}
\end{aligned}$$

Now we start with the inner sum. Note that:

$$\sum_{0 \leq b < d} e^{i2\pi mb/d} = d \text{ if } d \mid m \text{ and } 0 \text{ otherwise.}$$

We now do a change of variables to rewrite the formula for $T_{2k}(n)f$ as:

$$(T_{2k}(n)f)(\tau) = \sum_{m \in \mathbb{Z}} \sum_{ad=n; a \geq 1} a^{2k-1} e^{i2\pi ma\tau} c(mn/a).$$

This comes from using the substitution $md \mapsto mn/a$ and by using the fact that we can only focus on the terms where $d \mid m$ from the previous note. Next, we collect like powers of $e^{i2\pi\tau}$ to get that

$$(T_{2k}(n)f)(\tau) = \sum_{m \in \mathbb{Z}} \sum_{a \mid \gcd(M, n)} a^{2k-1} c(Mn/a^2) e^{i2\pi M\tau}$$

where $M = ma$. This exactly matches up to how we wanted to describe the coefficients so we have completed the proof. \square

We use these lemmas as we go about proving the following theorem.

Theorem 2. *Let f be a modular function (respectively modular form, respectively cusp form) of weight $2k$. Then so is $T_{2k}(n)f$.*

Proof. The first thing we need to show is that $T_{2k}(n)f$ has weight $2k$. From the previous Lemma 1 we get that $T_{2k}(n)f$ is associated to $T(n)F_f$. So:

$$\begin{aligned}
(T(n)F)(\lambda\Lambda) &= \sum_{\Lambda' \overset{n}{\subset} \lambda\Lambda} F(\Lambda') = \sum_{\Lambda' \overset{n}{\subset} \Lambda} F(\lambda\Lambda') \\
&= \lambda^{-2k} \sum_{\Lambda' \overset{n}{\subset} \Lambda} F(\Lambda') = \lambda^{-2k} (T(n)F)(\Lambda).
\end{aligned}$$

Now, we recall the following formula:

$$(T_{2k}(n)f)(\tau) = n^{2k-1} \sum_{\substack{ad=n; a \geq 1 \\ 0 \leq b < d}} d^{-2k} f\left(\frac{a\tau + b}{d}\right).$$

From here we can see that since f is meromorphic on \mathbb{H} that we also have $T(n)f$ being meromorphic on \mathbb{H} . This is because $T(n)f$ is just a sum of a whole lot of functions that are meromorphic on \mathbb{H} and so the full sum must also be meromorphic on \mathbb{H} .

Finally, we turn to looking at $T_{2k}(n)f$ at ∞ . We look at the above Lemma 3 concerning the coefficients. First, we see that $\gamma(0) = c(0)\sigma_{2k-1}(n)$, $\gamma(1) = c(n)$ and for primes that $\gamma(p) = c(pn) + p^{2k-1}c(n/p)$ if $p \mid n$ and just $\gamma(p) = c(pn)$ if $p \nmid n$. Basically from this we see that since $c(m) = 0$ for $m \leq -m_0 \leq 0$ then we know that $\gamma(m) = 0$ for $m \leq -m_0n$ because $\gamma(m)$ depends on $c(mn/a^2)$ with $a \mid \gcd(m, n)$. But if $a \mid \gcd(m, n)$ then we must have $mn/a^2 \leq -m_0$. So we then get that $T_{2k}(n)f$ will be meromorphic at ∞ if f is. \square

The important thing here is to see how the coefficients of the Fourier series for $T_{2k}(n)$ behave. We see the relationship between these two objects in the following theorem.

Theorem 3. *Let $f(\tau) = \sum (m)q^m \neq 0$ be a cusp form of weight $2k$, and suppose that f is an eigenfunction for all Hecke operators $T_{2k}(n)$, say $T_{2k}(n)f = \lambda(n)f$. Then we get that $c(1) \neq 0$ and $c(n) = \lambda(n)c(1)$ for all $n \geq 1$.*

Proof. We look at coefficients. First, we get that $T_{2k}(n)f = c(n)q + \dots$ and next, we get that $\lambda(n)f = \lambda(n)c(1)q + \dots$ where we are only caring about the leading term. From here we get that $c(n) = \lambda(n)c(1)$ which is exactly what we wanted in the second part of the theorem.

Now assume that $c(1) = 0$. But then we get that

$$c(n) = \lambda(n)c(1) = \lambda(n) \times 0 = 0$$

for all $n \geq 1$ and so $f \equiv 0$. But we assumed that $f \neq 0$ so this is a contradiction. Thus we cannot have $c(1) = 0$. \square

Definition 16. *From above we can get a special kind of eigenfunction. A simultaneous eigenfunction is called normalized if $c(1) = 1$.*

Note that when we couple the previous Theorem 3 with the above definition we get that every simultaneous eigenfunction is a constant multiple of a normalized eigenfunction.

Now, we remember Theorem 1 which gave some specific identities for when $T(n)$ acted on lattices \mathcal{L} . From what we have shown since then we can relate new equations.

Theorem 4. *Let f be a (weakly) modular function of weight $2k$.*

1. $T_{2k}(mn)f = T_{2k}(m)T_{2k}(n)f$ for all $m, n \in \mathbb{Z}$ with $\gcd(m, n) = 1$.
2. $T_{2k}(p^e)T_{2k}(p)f = T_{2k}(p^{e+1})f + p^{2k-1}T_{2k}(p^{e-1})f$ for all primes p and all $e \geq 1$.

Proof. 1. Recall Theorem 1, part 3. This directly follows.

2. Recall Theorem 1, part 4 and Lemma 1. Combining these we get the desired result. So:

$$R_\lambda F_f(\Lambda) = F_f(\lambda\Lambda) = \lambda^{-2k} F_f(\Lambda)$$

and thus:

$$\begin{aligned} T(p^e)T(p)F_f &= T(p^{e+1})F_f + pT(p^{e-1})R_p F_f \\ &= T(p^{e+1})F_f + pT(p^{e-1})p^{-2k}F_f \\ &= T(p^{e+1})F_f + p^{2k-1}T(p^{e-1})F_f \end{aligned}$$

Multiplying through by $p^{(e+1)(2k-1)}$ and recalling that $T_{2k}(n)f = n^{2k-1}T(n)F_f$ gives the exact result:

$$(p^{(e+1)(2k-1)})(T(p^e)T(p)F_f) = T_{2k}(p^{e+1})F_f = T_{2k}(p^e)T_{2k}(p)F_f \quad \text{and}$$

$$\begin{aligned} (p^{(e+1)(2k-1)})(T(p^{e+1})F_f + p^{2k-1}T(p^{e-1})F_f) &= \\ T_{2k}(p^{e+1})f + p^{2k-1}T_{2k}(p^{e-1})f. \end{aligned}$$

□

Corollary 3. Let $f(\tau) = \sum c(n)q^n \neq 0$ be a cusp form of weight $2k$ that is a normalized eigenfunction for every Hecke operator $T_{2k}(n)$. Then:

1. $c(mn) = c(m)c(n)$ for all $m, n \in \mathbb{Z}$ with $\gcd(m, n) = 1$.
2. $c(p^e)c(p) = c(p^{e+1}) + p^{2k-1}c(p^{e-1})$ for all primes p and $e \geq 1$.

Finally, we approach what we have set out to prove from the beginning: the above identities can lead us to an Euler product for a specific Dirichlet series attached to f . But first, one last definition for this section.

Definition 17. For any power series

$$f = \sum_{n \geq 1} c(n)q^n \in \mathbb{C}[[q]],$$

the L -series attached to f is the (formal) Dirichlet series

$$L(f, s) = \sum_{n \geq 1} c(n)n^{-s}.$$

Theorem 5. Let $f = \sum_{n \geq 1} c(n)q^n$ be a power series with $c(1) = 1$. Then the coefficients of f satisfy the following:

1. $c(mn) = c(m)c(n)$ for all m, n with $\gcd(m, n) = 1$ and

2. $c(p^e)c(p) = c(p^{e+1}) + p^{2k-1}c(p^{e-1})$ for primes p and $e \geq 1$

if and only if the associated L -function $L(f, s)$ has the Euler product expansion.

$$L(f, s) = \prod_p \frac{1}{1 - c(p)p^{-s} + p^{2k-1-2s}}.$$

Proof. First assume that (1) and (2) hold since what we are striving for in this section is the Euler product. Now, from (1) we can actually break $L(f, s)$ down into a product of primes like so:

$$L(f, s) = \sum_{n \geq 1} c(n)n^{-s} = \prod_p \sum_{e \geq 0} c(p^e)p^{-es}.$$

We now do some algebra:

$$\begin{aligned} & (1 - c(p)p^{-s} + p^{2k-1-2s}) \left(\sum_{e \geq 0} c(p^e)p^{-es} \right) \\ &= \sum_{e \geq 0} c(p^e)p^{-es} - \sum_{e \geq 0} c(p)c(p^e)p^{-(e+1)s} + \sum_{e \geq 0} c(p^e)p^{2k-1-(e+2)s} \\ &= \{c(1) + c(p)p^{-s}\} - \{c(p)c(1)p^{-s}\} \\ &\quad + \sum_{e \geq 2} (c(p^e) - c(p)c(p^{e-1}) + c(p^{e-2})p^{2k-1})p^{-es} \\ &= 1 \end{aligned}$$

The reason this all reduced to just 1 was two-fold. First we use that $c(1) = 1$ to get $\{c(1) + c(p)p^{-s}\} - \{c(p)c(1)p^{-s}\} = 1 + c(p)p^{-s} - c(p)*1*p^{-s} = 1$. Next we use (2) to look at the sum part and see that $c(p^e) - c(p)c(p^{e-1}) + c(p^{e-2})p^{2k-1} = 0$ since (after rearranging (2) to get symmetry) $c(p^{e+1}) = c(p^e)c(p) - c(p^{e-1})p^{2k-1}$. So, using this we get that:

$$\sum_{e \geq 0} c(p^e)p^{-es} = \frac{1}{1 - c(p)p^{-s} + p^{2k-1-2s}},$$

which is exactly the Euler product we have been wanting all along. \square

5 The Analytic Properties

This chapter will highlight the remaining properties for an L -function to be in the Selberg Class. First, however, we need to give a lemma.

Lemma 4. (Hecke) Let $f(\tau)$ be a cusp form of weight $2k$ with Fourier expansion $\sum c(n)q^n$. There is a constant κ , depending only on f , such that $|c(n)| \leq \kappa n^k$ for all $n \geq 1$.

Proof. Note that we have a formula for the n^{th} Fourier coefficient of f :

$$c(n) = \int_0^1 e^{-i2\pi n(x+iy)} f(x+iy) dx.$$

Therefore we have:

$$|c(n)| \leq e^{2\pi ny} \sup_{0 \leq x \leq 1} |f(x+iy)|.$$

Now introduce the following real-valued function:

$$\phi(\tau) = |f(\tau)|(\text{Im}\tau)^k.$$

We first note about $\phi(\tau)$ that $\phi(\gamma\tau) = \phi(\tau)$ for all $\gamma \in \Gamma(1)$. Further, it turns out that for the values in \mathbb{H} that we care about (the fundamental domain of $\Gamma(1) \backslash \mathbb{H}$), that we can actually get a bound on $\sup \phi(\tau)$, thus we can denote $C = \sup_{\tau \in \mathbb{H}} \phi(\tau)$. Therefore:

$$|f(x+iy)| = \phi(x+iy)y^{-k} \leq Cy^{-k} \quad \text{for all } x+iy \in \mathbb{H}.$$

We plug this back into our formula for $|c(n)|$ to get that $|c(n)| \leq Cy^{-k}e^{2\pi ny}$. Since this is valid for all $y > 0$, we can say $y = 1/n$ to get our result, namely:

$$|c(n)| = C \left(\frac{1}{n}\right)^{-k} e^{2\pi n(1/n)} = Cn^k e^{2\pi} = \kappa n^k.$$

□

We now use this lemma to go about proving both the analytic continuation and functional equation properties in one theorem:

Theorem 6. *Let $f(\tau)$ be a cusp form of weight $2k$. Then:*

1. $L(f, s)$ has an analytic continuation to all of \mathbb{C} .
2. If

$$R(f, s) = (2\pi)^{-s} \Gamma(s) L(f, s) \quad \text{then} \quad R(f, 2k-s) = (-1)^k R(f, s)$$

for all $s \in \mathbb{C}$.

Proof. Recall that

$$\Gamma(s) = \int_0^\infty t^{s-1} e^{-t} dt \quad \text{for } \text{Re}(s) > 0.$$

Now do a substitution of $t \mapsto 2\pi nt$ to get:

$$n^{-s} = (2\pi)^s \Gamma(s)^{-1} \int_0^\infty t^{s-1} e^{-2\pi nt} dt.$$

Now, let $f(\tau) = \sum c(n)q^n$ and we see that:

$$\begin{aligned} L(f, s) &= \sum_{n \geq 1} c(n)n^{-s} = \sum_{n \geq 1} \{c(n)(2\pi)^s \Gamma(s)^{-1} \int_0^\infty t^{s-1} e^{-2\pi n t} dt\} \\ &= (2\pi)^s \Gamma(s)^{-1} \int_0^\infty t^{s-1} \sum_{n \geq 1} c(n) e^{-2\pi n t} dt \\ &= (2\pi)^s \Gamma(s)^{-1} \int_0^\infty t^{s-1} f(it) dt. \end{aligned}$$

Now, the important thing to see here is to recall the above Lemma 4. There we showed that $|c(n)| \leq \kappa n^k$. This is why it was allowed for us to move the above sum inside the integral (occurring from the first line to the second line).

Now, we separate our integral into two parts, for $0 \leq t \leq 1$ and for $1 \leq t \leq \infty$. We also recall that f has the following property:

$$f\left(\frac{i}{t}\right) = (it)^{2k} f(it).$$

Thus, after rearranging our terms we have:

$$\begin{aligned} (2\pi)^{-s} \Gamma(s) L(f, s) &= \int_0^\infty t^{s-1} f(it) dt \\ &= \int_0^1 t^{s-1} f(it) dt + \int_1^\infty t^{s-1} f(it) dt \\ &= \int_1^0 \left(\frac{1}{t}\right)^{s-1} f\left(\frac{i}{t}\right) d\left(\frac{1}{t}\right) + \int_1^\infty t^{s-1} f(it) dt \\ &= \int_1^\infty (-1)^k t^{2k-s-1} f(it) dt + \int_1^\infty t^{s-1} f(it) dt. \end{aligned}$$

We sum this all up as so:

$$L(f, s) = (2\pi)^s \Gamma(s)^{-1} \int_1^\infty \{t^{s-1} + (-1)^k t^{2k-s-1}\} f(it) dt \quad \text{for } \operatorname{Re}(s) > k + 1.$$

We have some notes to make on this equation. First, we know that $\Gamma(s)^{-1}$ is holomorphic on \mathbb{C} . Second we know that the integral above is absolutely convergent for s in any compact subset of \mathbb{C} (this follows from f being a cusp form). Lastly, we note the following property:

$$\epsilon(s, t) = t^{s-1} + (-1)^k t^{2k-s-1} \quad \text{satisfies} \quad \epsilon(2k-s, t) = (-1)^k \epsilon(s, t).$$

So now we give the following relation:

$$\text{If } R(f, s) = (2\pi)^{-s} \Gamma(s) L(f, s) = \int_1^\infty \epsilon(s, t) f(it) dt, \quad \text{then}$$

$$R(f, 2k-s) = (-1)^k R(f, s).$$

This is really close to what we want. We actually want a relationship between $R(f, s)$ and $R(f, 1 - s)$ though so we need to do a change of variables. We do this by using the map $s \mapsto s + (k - 1/2)$. This is how this works out. First we see that:

$$R'(f, s) = R(f, s + (k - 1/2)).$$

Now we turn our attention to the other part of the functional equation:

$$\begin{aligned} R'(1 - s) &= R(f, 1 - s + (k - 1/2)) \\ &= (-1)^k \times R(f, 2k - (1 - s + (k - 1/2))) \\ &= (-1)^k \times R(f, s + k - 1/2) \\ &= (-1)^k \times R'(f, s) \end{aligned}$$

We now have the desired relationship between $R(f, s)$ and $R(f, 1 - s)$. So this finally gives us both properties that we want: analytic continuation and a functional equation. \square

This leaves the Ramanujan Hypothesis property left. For this we need to note a strong result.

Fact 1.

$$|a_n| \leq n^{k-1/2}$$

Proving this result goes beyond the scope of this paper so it will be taken as fact (for more information, see the references of Deligne). Now, we proceed by recalling that with our change of variables from above we get the following change to our L -function:

$$\begin{aligned} L'(s) &= \sum a_n n^{-(s+k-1/2)} \\ &= \sum \left(a_n n^{-k+1/2} \right) n^{-s} \\ &= \sum b_n n^{-s} \end{aligned}$$

By using this substitution we can see that $|b_n| \leq 1$ which is exactly what we needed to satisfy the Ramanujan-Hypothesis property.

6 Conclusion

So we can now look back on everything we have showed. We started off with some preliminary definitions concerning elliptic curves, modular forms, and L -functions. We then tied these two objects together by looking at the L -function related to a modular form.

Next came the bulk of the paper where we showed that this L -function belongs to a special class of L -functions called the Selberg Class. As it turned out we needed to show five properties. The first, dealing with the convergence of the series was handled immediately by our definitions. Next, we used Hecke

operators to handle the fourth property, that of an Euler product. It turned out that this was actually where most of the work for the paper lied. The three remaining properties were all analytic in nature and were handled in one section.

So why is it important that the L -function for a modular form is a member of the Selberg Class? As it turns out, the Selberg Class is really quite a recent formation (from the early 1990s) and thus there are quite a few open problems and conjectures here. Next, the Selberg Class L -functions tend to be very "standard" L -functions. Hence, by understanding them we can hope to gain insight on all other L -functions. Naturally, any result on L -functions will lead to further understanding of both the Riemann equation and hence primes in general which is always important.

References

- [1] Conrad, Keith. Class Lecture. Arithmetic of L -functions. Park City Mathematics Institute, Park City, UT. July 2009.
- [2] Deligne, Pierre. "Formes modulaires et représentations l -adiques", Séminaire Bourbaki vol. 1968/69 Exposés 347-363, Lecture Notes in Mathematics, 179, Berlin, New York: Springer-Verlag.
- [3] Deligne, Pierre. La conjecture de Weil: I. Publications Mathématiques de l'IHÉS, 43 (1974), p. 273-307.
- [4] Helm, David. Class Lecture. Conference Course. The University of Texas at Austin, Austin, TX. Spring 2010.
- [5] Murty, M. Ram, *Problems in Analytic Number Theory*, Springer, New York, 2008.
- [6] Serre, Jean-Pierre, *A Course in Arithmetic*, Springer-Verlag, New York, 1973.
- [7] Silverman, Joseph H., *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1994.
- [8] Silverman, Joseph H. and John Tate, *Rational Points on Elliptic Curves*, Springer, New York, 1992.
- [9] Vaaler, Jeffrey. Class Lecture. Honors Tutorial Course. The University of Texas at Austin, Austin, TX. Fall 2009.
- [10] Voloch, Felipe. Class Lecture. Elliptic Curves. The University of Texas at Austin, Austin, TX. 19 January 2010.